Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ONLINE
23 i 24 czerwca 2026 r.

OCHRONA INFORMACJI NIEJAWNYCH W JEDNOSTCE: FUNKCJONOWANIE KANCELARII TAJNEJ ORAZ KANCELARII MATERIAŁÓW NIEJAWNYCH – ŚRODKI BEZPIECZEŃSTWA, OBIEG MATERIAŁÓW, PRAKTYCZNE STOSOWANIE PRZEPISÓW

WAŻNE INFORMACJE:

- Skuteczna ochrona informacji niejawnych stanowi jeden z kluczowych elementów systemu bezpieczeństwa państwa oraz prawidłowego funkcjonowania jednostek sektora finansów publicznych. **W warunkach rosnących zagrożeń związanych z działalnością obcych służb wywiadowczych, cyberzagrożeniami oraz koniecznością zapewnienia ciągłości działania administracji publicznej, szczególnego znaczenia nabiera właściwa organizacja systemu ochrony informacji niejawnych oraz bezpieczeństwa teleinformatycznego.**
- Prawidłowe wdrożenie i stosowanie procedur związanych z ochroną informacji niejawnych wymaga nie tylko znajomości aktualnych przepisów prawa, ale również umiejętności praktycznego organizowania procesów bezpieczeństwa w jednostce organizacyjnej. Istotną rolę odgrywa także **odpowiednie przygotowanie dokumentacji, właściwe funkcjonowanie pionu ochrony, kancelarii tajnych oraz zapewnienie skutecznych środków bezpieczeństwa fizycznego i teleinformatycznego.**
- Program obejmuje **zarówno zagadnienia systemowe i prawne, jak i praktyczne aspekty organizacji ochrony informacji niejawnych, funkcjonowania kancelarii tajnych, bezpieczeństwa teleinformatycznego oraz odpowiedzialności związanej z naruszeniem przepisów o ochronie informacji niejawnych.**
- Zajęcia polecamy osobom, które od niedawna zajmują się tą tematyką, jak i osobom z dłuższym stażem, które chcą rozwiązać problemy, zdobyć wiedzę oraz uchronić się przed nieprawidłowościami dotyczącymi prawidłowej organizacji pracy oraz ochrony informacji niejawnych w jednostce.

CELE I KORZYŚCI ZE SZKOLENIA:

- Usystematyzowanie i aktualizacja wiedzy uczestników w zakresie organizacji systemu ochrony informacji niejawnych oraz obowiązków jednostek sektora finansów publicznych wynikających z obowiązujących przepisów prawa.
- Podniesienie kompetencji pracowników, **odpowiedzialnych za ochronę informacji niejawnych, bezpieczeństwo teleinformatyczne oraz realizację zadań związanych z zarządzaniem kryzysowym i bezpieczeństwem organizacyjnym jednostki.**
- Przekazanie praktycznej wiedzy dotyczącej **tworzenia, wdrażania i aktualizacji dokumentacji związanej z ochroną informacji niejawnych, w tym planów ochrony, instrukcji bezpieczeństwa oraz zasad obiegu dokumentów niejawnych.**
- Przedstawienie zasad organizacji **kancelarii tajnych, stosowania środków bezpieczeństwa fizycznego i teleinformatycznego oraz wymagań dotyczących personelu pionu ochrony.**
- Poznanie podstawowych metod stosowania środków bezpieczeństwa fizycznego, tak, aby skutecznie zabezpieczyć posiadane informacje niejawne, racjonalnie gospodarując przy tym środkami finansowymi.
- Zwiększenie świadomości w zakresie **zagrożeń dla bezpieczeństwa informacji, odpowiedzialności służbowej, dyscyplinarnej i karnej oraz sposobów minimalizowania ryzyk związanych z nieuprawnionym ujawnieniem informacji niejawnych.**

- Rozwinięcie praktycznych umiejętności uczestników w zakresie stosowania procedur ochrony informacji niejawnych, współpracy z przedsiębiorcami, posiadającymi dostęp do informacji niejawnych oraz zapewnienia zgodności działań jednostki z wymogami bezpieczeństwa i przepisami prawa.

PROGRAM:

I dzień – 23 czerwca 2026 r. Podstawy ochrony informacji niejawnych.

1. Aktualne zagrożenia związane z działalnością obcych służb wywiadowczych.
2. System ochrony informacji niejawnych w RP - tajemnice prawnie chronione w Polsce.
3. Aktualne podstawy prawne ochrony informacji niejawnych - przepisy ogólne i resortowe.
4. Nadzór nad systemem ochrony informacji niejawnych w Polsce:
   - Kolegium ds. Służb Specjalnych.
   - Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego.
5. Rola i zadania Kierownika Jednostki Organizacyjnej związane z zapewnieniem ochrony informacji niejawnych.
6. Pion ochrony w jednostce organizacyjnej – struktura i wymagania formalne wobec personelu:
   - Pełnomocnik ochrony.
   - Kierownik Kancelarii Tajnej (Kancelarii Materiałów Niejawnych).
   - Inspektor Bezpieczeństwa Teleinformatycznego.
   - Administrator Systemu.
   - Pozostali pracownicy pionu ochrony.
7. Ochrona informacji niejawnych w stosunkach międzynarodowych. Krajowa Władza Bezpieczeństwa.
8. System kancelarii tajnych w RP oraz kancelarii tajnych międzynarodowych.
9. Obowiązki informacyjne Kierownika Jednostki Organizacyjnej związane z utworzeniem lub likwidacją Kancelarii Tajnej.
10. Wymagana dokumentacja związana z utworzeniem kancelarii oraz zapewnieniem obiegu informacji niejawnych w podmiocie:
    - Ocena poziomu zagrożeń.
    - Instrukcja dotyczącą sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „Zastrzeżone” oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.
    - Instrukcja przetwarzania informacji niejawnych o klauzuli „Poufne”.
    - Plan ochrony informacji niejawnych.
    - Zasady obiegu dokumentów o klauzuli „Tajne” lub wyższej.
    - Ewidencje prowadzone przez Pełnomocnika Ochrony.
    - Zasady punktacji środków bezpieczeństwa fizycznego. Normy mające zastosowanie przy ochronie informacji niejawnych.
11. Omówienie typowych środków bezpieczeństwa stosowanych do ochrony informacji niejawnych w Kancelarii Tajnej i Kancelarii Materiałów Niejawnych:
    - Strefy ochronne.
    - Szafy metalowe oraz meble biurowe.
    - Pomieszczenia oraz zamki, ściany i stropy, drzwi i okna.
    - System Kontroli Dostępu.
    - Personel bezpieczeństwa.
    - System Sygnalizacji Włamania i Napadu.
    - Monitoring wizyjny.
12. Certyfikacja środków bezpieczeństwa fizycznego.

II dzień – 24 czerwca 2026 r. Praktyczne zagadnienia związane z organizacją ochrony informacji niejawnych w jednostce organizacyjnej.

1. Archiwizacja materiałów niejawnych – zdawanie dokumentów do własnego archiwum zakładowego (składnicy akta) lub ich przekazanie do archiwów państwowych.
2. Zasady dostępu do informacji niejawnych przez przedsiębiorców:
   - Kwestionariusz bezpieczeństwa przemysłowego.
   - Świadectwa bezpieczeństwa przemysłowego – rodzaje i terminy ważności.
   - Podstawowe wymagania związane z zawieraniem z przedsiębiorcami umów, których realizacja wiąże się z dostępem do informacji niejawnych.
3. RODO a ochrona informacji niejawnych.
4. Informacje niejawne a prawo dostępu do informacji publicznej.
5. Bezpieczeństwo teleinformatyczne:
   - Przetwarzanie informacji niejawnych w systemach i sieciach teleinformatycznych. Zasady ogólne.
   - Personel bezpieczeństwa - Administrator systemu i Inspektor Bezpieczeństwa Teleinformatycznego – wymagania formalne, rola i zadania.
   - Akredytacja systemów teleinformatycznych służących do przetwarzania informacji niejawnych.
   - Dokumentacja bezpieczeństwa teleinformatycznego - Szczególne Wymagania Bezpieczeństwa Systemu oraz Procedury Bezpiecznej Eksploatacji.
   - Środki bezpieczeństwa fizycznego stosowane w celu ochrony systemów i sieci przetwarzających informacje niejawne.
   - Sprzętowa Strefa Ochrony Elektromagnetycznej.
   - Brakowanie nośników informatycznych służących do przetwarzania materiałów niejawnych.
6. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów:
   - Odpowiedzialność dyscyplinarna za niezachowanie należytej staranności przy ochronie informacji.
   - Kodeks pracy – obowiązki i odpowiedzialność pracownika w zakresie przestrzegania tajemnicy.
   - Kodeks karny – przestępstwa przeciwko ochronie informacji.
7. Wymiana doświadczeń i konsultacje, odpowiedzi na pytania uczestników.

ADRESACI:

Kadra zarządzająca, sekretarze w jednostkach samorządu terytorialnego, pełnomocnicy ds. ochrony informacji niejawnych w instytucjach publicznych, osoby odpowiedzialne za rejestrację i obieg dokumentów niejawnych/ kierownicy Kancelarii Materiałów Niejawnych, pracownicy komórek zarządzania kryzysowego i OC, pracownicy komórek organizacyjnych, odpowiedzialni w jednostce za ochronę informacji niejawnych.

PROWADZĄCY:

certyfikowany Inspektor Ochrony Danych, Menedżer Bezpieczeństwa Informacji oraz Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji. W latach 1992 - 2013 funkcjonariusz UOP/ABW, od 1999r. zajmuje się problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009r. ekspert ABW z zakresu OIN. Współorganizator szkoleń i konferencji poświęconych problematyce ochrony informacji oraz danych osobowych. W latach 2013 - 2017 Pełnomocnik ds. ochrony informacji niejawnych w Urzędzie Wojewódzkim oraz innych jednostkach, absolwent UMK w Toruniu oraz studiów podyplomowych WSAiB w Gdyni na kierunku zarządzanie bezpieczeństwem informacji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Ochrona informacji niejawnych w jednostce: funkcjonowanie Kancelarii Tajnej oraz Kancelarii Materiałów Niejawnych – środki bezpieczeństwa, obieg materiałów, praktyczne stosowanie przepisów

	Szkolenie będziemy realizowali **w formie webinarium online**.
	23 i 24 czerwca 2026 r. **Szkolenie w godzinach 9:00-13:00**
	Cena: 769 PLN netto/os. Przy zgłoszeniu do **9 czerwca 2026 r.** cena wynosi: **739 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.
CENA zawiera:	udział w profesjonalnym szkoleniu oline z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego ośrodek regionalny w Rzeszowie, Podkarpacki Ośrodek Samorządu Terytorialnego 35 – 073 Rzeszów, ul. Kolejowa 1, tel. 17 862 69 64 post@frdl.rzeszow.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

(dane do faktury)
Nazwa i adres nabywcy
NIP Nabywcy

Nazwa i adres odbiorcy
NIP Odbiorcy

NIP **Telefon**

1. **Imię i nazwisko uczestnika,** stanowisko,
   E-MAIL i TEL. DO KONTAKTU
2. **Imię i nazwisko uczestnika,** stanowisko,
   E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe) TAK ☐ NIE ☐

Faktura zostanie wystawiona jako faktura ustrukturyzowana w Krajowym Systemie e-Faktur (KSeF).
Uwagi: ……

Proszę o przesłanie certyfikatu na adres mailowy: ……

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora www.frdl.rzeszow.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.rzeszow.pl do 18 czerwca 2026 r.

UWAGA! Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie faktury w KSeF.

Podpis osoby upoważnionej _____